CLAIMS

What is Claimed is:

1. A method comprising:

emulating a SMTP client application comprising generating at least one SMTP client application dirty page;

emulating an executable application sent from said SMTP client application comprising generating at least one executable application dirty page; and

determining whether said at least one SMTP client application dirty page is a match of said at least one executable application dirty page.

2. The method of Claim 1 further comprising establishing a SMTP proxy, wherein said SMTP client application forms a connection with said SMTP proxy.

3. The method of Claim 1 further comprising determining whether SMTP client application dirty pages were generated during said emulating a SMTP client application, said SMTP client application dirty pages comprising said at least one SMTP client application dirty page.

4. The method of Claim 3 further comprising saving a state of said SMTP client application upon a determination that said SMTP client application dirty pages were generated during said emulating a SMTP client application.

5. The method of Claim 1 wherein said SMTP client application sends data comprising said executable application.

6. The method of Claim 5 further comprising decomposing said data.

7. The method of Claim 5 further comprising determining whether said data comprises executable content.

8. The method of Claim 5 further comprising establishing a SMTP proxy, wherein said data is intercepted and stalled by said SMTP proxy.

9. The method of Claim 5 further comprising stalling said data.

10. The method of Claim 9 wherein upon a determination that said at least one SMTP client application dirty page is not a match of said at least one executable application dirty page, said method further comprising allowing said data to proceed.

11. The method of Claim 9 wherein upon a determination that said at least one SMTP client application dirty page is a match of said at least one executable application dirty page, said method further comprising taking protective action to protect a computer system.

12. The method of Claim 11 further comprising determining that said match is not a known false positive prior to said taking protective action.

13. The method of Claim 11 further comprising providing a notification of said protective action.

14. The method of Claim 5 further comprising determining whether said data comprises executable applications that have not been emulated.

15. The method of Claim 14 wherein upon a determination that said data does comprised executable applications that have not been emulated, said method further comprising selecting a next executable application for emulation.

16. The method of Claim 15 further comprising emulating said next executable application.

17. The method of Claim 1 further comprising determining whether executable application dirty pages were generated during said emulating an executable application, said executable application dirty pages comprising said at least one executable application dirty page.

18. The method of Claim 1 wherein said SMTP client application is a polymorphic malicious code.

19. A method comprising:

emulating a SMTP client application;

determining whether SMTP client application dirty pages were generated during said emulating a SMTP client application;

excluding said SMTP client application as a polymorphic malicious code upon a determination that said SMTP client application dirty pages were not generated; and

saving a state of said SMTP client application upon a determination that said SMTP client application dirty pages were generated.

20. The method of Claim 19 further comprising:

stalling data from said SMTP client application;

determining whether said SMTP client application is excluded as said polymorphic malicious code; and

allowing said data to proceed upon a determination that said SMTP client application is excluded.

21. A computer program product comprising a polymorphic worm blocking application, said polymorphic worm blocking application for:

emulating a SMTP client application comprising generating at least one SMTP client application dirty page;

emulating an executable application sent from said SMTP client application comprising generating at least one executable application dirty page; and

determining whether said at least one SMTP client application dirty page is a match of said at least one executable application dirty page.

22. A method comprising:

establishing a SMTP proxy;

defining an application that forms a connection with said SMTP proxy as a SMTP client application;

decrypting said SMTP client application;

intercepting an executable application sent from said SMTP client application with said SMTP proxy;

decrypting said executable application; and

determining whether said SMTP client application when decrypted is the same as said executable application when decrypted.